

UNITED STATES DISTRICT COURT

for the
District of Nebraska

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Case No. 8:22MJ480

One (1) Black Samsung cellular telephone with IMEI number 350319813108941.

The device is currently located in the FBI Omaha Field Office, 4411 S.121st

Street, Omaha, Nebraska 68137, further described in Attachment A

APPLICATION FOR A SEARCH WARRANT

At the request of an attorney for the government, I state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

One (1) Black Samsung cellular telephone with IMEI number 350319813108941 The device is currently located in the FBI Omaha Field Office, 4411 S 121st Street, Omaha, Nebraska 68137, further described in Attachment A

located in the _____ District of _____ Nebraska _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2251(a)	Sexual exploitation of children
18 U.S.C. § 2252(a)(2), 2252A(a)(2)(A)	Receipt and distribution of child pornography
18 U.S.C. § 2252(a)(1)	Transportation of child pornography
18 U.S.C. § 2252(a)(4)(B), 2252A(a)(5)(B), (b)(2)	Possession of child pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

This application and affidavit were presented by an attorney for the government.



Applicant's signature

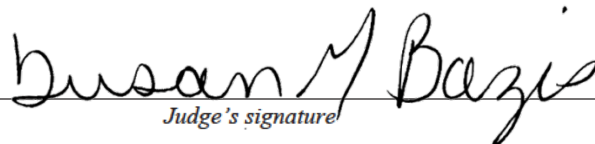
- ☐ Sworn to before me and signed in my presence.

Timothy DuBois, SA, FBI

Printed name and title

- ☒ Sworn to before me by telephone or other reliable electronic means.

Date: 8-26-22



Judge's signature

City and state: Omaha, Nebraska

SUSAN M. BAZIS, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

IN THE MATTER OF THE SEARCH OF
One (1) Black Samsung cellular telephone
with IMEI number 350319813108941
CURRENTLY LOCATED AT THE **FBI**
OMAHA FIELD OFFICE 4411 S. 121st
Street, Omaha, Nebraska 68137

Case No. 8:22MJ480

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Timothy DuBois, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI), and have been so employed since November of 2021. I am currently assigned to the FBI Omaha Division, where I am responsible for investigating violations of various criminal statutes, including those pertaining to Possession of Child Pornography, in violation of Title 18, United States Code 2252(a)(4)(B) & (b)(2), and Production of Child Pornography Title 18, United States Code, Section 2251(a) & (e). I have assisted in child pornography and child exploitation investigations, which have resulted in search warrants, arrests, and the seizure and forfeiture of assets.

3. I have received relevant training in child pornography and child exploitation investigations from the FBI Academy in Quantico, Virginia. I have also acquired knowledge and information about the means and methods of child pornography and child exploitation investigations, to include informal training, interaction with other law enforcement officers and investigators, informants, persons whom I have arrested and/or interviewed, and my participation in multiple investigations related to child pornography and child exploitation investigations. The aforementioned investigations ultimately led to the arrests and convictions of those persons who violated those federal crimes.

4. Based on my training, experience, and investigation, your affiant developed probable cause to believe, and does believe that evidence relative to proving the crimes described herein is secured or being kept at or within the following described device. I have probable cause to believe that the device to be searched, as described in Attachment A, will contain evidence, as described in Attachment B, of violations of federal law, including 18 U.S.C. § 2251(a) (sexual exploitation of children), 18 U.S.C. § 2252(a)(2) (receipt and distribution of child pornography), 18 U.S.C. § 2252(a)(1) (transportation of child pornography), 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2252A(a)(2)(A) (receipt and distribution of child pornography)

5. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement officers, other personnel specially trained in the seizure and analysis of computers and electronic media, and on my experience and training as an FBI Agent. Because this affidavit is being submitted for the limited purpose of securing a search warrant, your affiant has not included each and every fact known to me concerning this investigation. Your affiant has set forth only the facts that he believes are necessary to establish probable cause to believe that evidence of a violation of 18 U.S.C. § 2251(a) (sexual exploitation

of children), 18 U.S.C. § 2252(a)(2) (receipt and distribution of child pornography), 18 U.S.C. § 2252(a)(1) (transportation of child pornography), 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography), 2252A(a)(5)(B) and (b)(2) (possession of child pornography), and 2252A(a)(2)(A) (receipt and distribution of child pornography) exists and is stored in the TARGET DEVICE, which is described in Attachment A of this affidavit.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. The property to be searched is **one (1) Black Samsung cellular telephone with IMEI number 350319813108941**. The device is currently located in the FBI Field Office, 4411 S.121st Street, Omaha, Nebraska 68137.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

8. SA Timothy DuBois was made aware of an investigation conducted by Neenah Wisconsin Police Department Investigator Craig Hoffer (hereinafter UCO). SA DuBois reviewed the investigative reports which are briefly summarized below. I have included only those details which I believe necessary to give an overview of the investigation and establish probable cause for the issuance of a search warrant for the electronic device currently being lawfully held in evidence.

9. UCO's reports stated that on September 10, 2019 he was operating in an undercover capacity on the social media dating app Joyride. UCO was contacted by an individual by the name of Hagendaz069. UCO had created a profile in which his persona was a fifteen-year-old female and this information was clearly disclosed to Hagendaz069 during the course of

their conversations. The conversations between UCO and Hagendaz069 were often sexual in nature and Hagendaz069 sent multiple images to the UCO one of which was his fully erect penis in his underwear. Hagendaz069 told the UCO that his snapchat username was also Hagendaz069. To positively identify Hagendaz069, UCO drafted a search warrant for the SnapChat account Hagendaz069. The search warrant which was signed by the Honorable Judge Daniel Bissett of the Winnebago County Circuit Court, Branch 6 located in the state of Wisconsin. On November 19, 2020 UCO received results back from Snapchat and identified Hagendaz069 to be Gerald Lawrence Vonruden, Date of birth June 18, 1969.

10. UCO completed a Request for Prosecution form which requested that an arrest warrant be issued for Gerald Vonruden DOB June 18, 1969. The charges spelled out on the arrest warrant were State of Wisconsin charges 948.055 (1) causing a child to view or listen to sexual activity, and 948.075 (1) use of a computer to facilitate a Child Sex Crime. On April 28, 2021, while Vonruden was traveling north on I29 near exit 61 in the state of Iowa, he was pulled over by Iowa State Trooper Rose Ives because the taillights on the vehicle he was driving were not functioning. During the stop, the Trooper found that Vonruden had a valid felony warrant and placed him under arrest. At the time of his arrest three devices were seized. They are a Black Samsung Galaxy S21 Ultra cellular phone, (Serial Number R5CR129QFGM), a Silver Verizon Samsung Tablet, and a Black Samsung Tablet (Serial number R52NA0DT7EZ). A search warrant was signed by the Honorable Judge Barbara Key, of the Winnebago County Circuit Court, Branch 3 on December 28, 2021 for the cell phone.

11. While reviewing the contents of the cell phone, UCO identified many items of evidence to include child pornography, the photo sent of Vonruden's fully erect penis in his underwear, and additional conversations with individuals who appear to be underage girls. Additionally, images of a prepubescent female were located on the phone in which it appears that

the child is photographed in a swimsuit in a mirror which appears to be voyeuristic, and close up photographs of the child's clothed legs and pelvis.

12. The contents of the cell phone included conversations conducted via Twitter. In a conversation with Twitter user "Kate" it appears that Vonruden purchased photos from her. Vonruden asks how old "Kate" was in some pictures that it appears he purchased from her. Kate replies stating "Most are pretty recent, so youngest is probably 15."

13. In a conversation with Twitter user "Polishbaby" it appears that "Polishbaby" is the father of a thirteen-year-old girl who he had been taking pictures of and sending to Vonruden. Vonruden and "Polishbaby" discuss engaging in sexual activity with the thirteen-year-old if Vonruden is in town.

14. In a conversation with Twitter user "Simon_Selwyn" Vonruden discusses sexual experiences that he has had with very young girls. Vonruden states: "My girlfriend has four nieces.. the middle 2.. youngest is a little brat like her mom not a turn on at all she's cute but pisses me off. One of them stayed overnight while her dad and son were on Boy Scout trip. Girlfriend was at work. We sleep naked and I knew she would be coming in to wake me up. I purposely left my bottom part of me out so she could see when she walked in. LOL. Hoping someday she's going to be staying overnight again:-) this is something I do all the time with her. Even when everybody's around. I put on these sports shorts you know the loose ones. She always loved to sit next to me or in front of me. And I have caught her looking. The couch and loveseat are recliners. I recline back put one leg up and when she's not looking I pull my shorts up to make sure she can completely see. And she looks so I know she can see. I can see you're out of the corner of my eye sneaking peeks"

15. Additionally, in the same conversation Vonruden states: "I have a younger picture of her but I can't find her right now. When she was younger than this we would play in the pool together because your dad has arthritis really bad so I would play. She would always put your

foot on my cock and rub it then she was like 9 years old. So this is a before picture

<https://t.co/pKLJM0k5Nd>”

16. On the Black Samsung Galaxy S21 Ultra (Serial Number R5CR129QFGM) cellular phone UCO found multiple images of Vonruden’s driver’s licenses, his passport, and images of him and his girlfriend.

17. SA DuBois has reviewed these items of evidence and approximately 80 images of Child Sexual Abuse Material (CSAM) were found. Four selected images are described below:

- a. Image “447c80886b0d8e46_0_embedded_1” depicts a male estimated to be roughly between the age of 8-12, based upon size and development, performing oral sex on a male estimated to be under the age of 13-17 years, old based upon size and development.
- b. Image “20200906_233824” of a prepubescent female estimated to be between the ages of 5-8 years old, based upon size and development, who is having oral sex performed on her by another prepubescent female estimated to be of a similar age, based upon size and development.
- c. Image “Screenshot_20190630-100156_Chrome” of two prepubescent females estimated to be between the ages of 8-12 years old, based upon size and development, posing fully nude with a swim toy in between them.
- d. Image “Screenshot_20191206-101334_Chrome” of a prepubescent female estimated to be between the ages of 7-12 years old, based upon size and development. Female is vaginally penetrated by a younger male with two younger males adjacent. Males appear to be minors, based upon size and development. Prepubescent female is grabbing the two adjacent males’ erect penises.

18. AUSA Alex Duros informed UCO on March 9, 2022 that he did not believe that there was enough information to charge Gerald Vonruden federally in the Eastern District of

Wisconsin because the child pornography which was recovered from Vonruden's cell phone was evidence that was seized when he was still in Iowa.

19. On June 14, 2022 search warrants for the two seized tablets were signed by the Honorable Magistrate Judge Susan M. Bazis in the District of Nebraska. SA DuBois was informed by FBI Omaha's Computer Analysis Response Team (CART) that they were only able to access one of the two tablets seized from Mr. Vonruden and make this device available for review. SA DuBois reviewed the contents of the unlocked Black Samsung tablet (Serial number R52NA0DT7EZ) and located approximately 100 additional images of CSAM on this device.

20. On August 4, 2022, a criminal complaint and arrest warrant for Gerald Vonruden regarding a violation of 18 USC 2252A(a)(4)(B), possession of Child Pornography, was signed by the Honorable Helen C. Adams, Chief U.S. Magistrate Judge for the Southern District of Iowa. Officers located and arrested Gerald Vonruden in Forest City, Iowa on August 18, 2022. At the time of the arrest Vonruden was in possession of a black Samsung cellular telephone bearing IMEI number 350319813108941 which is the target of this search warrant. According to transporting Agents, Vonruden made spontaneous utterances regarding doing things he should not have, and getting himself into trouble. Vonruden did not object to the arresting agents taking possession of his cell phone and stated that there was nothing on it and everything was on the phone already seized by the FBI.

21. Based on my training and experience, most individuals who seek out CSAM store it on multiple devices, collect images and videos, and seek to have frequent access to the material. Because of the fact that CSAM has been found on all of the devices in which law enforcement has been able to access, and the conversations in which Vonruden discusses his sexual interest in children, there is probable cause to believe that CSAM will also be located on

the device which is the target of this warrant. Your affiant respectfully requests a warrant be issued for the device described in Attachment A.

22. The device is currently located at the FBI Field Office, 4411 S.121st Street, Omaha, Nebraska 68137. In my training and experience, I know that the device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the devices first came into the possession of the FBI.

TECHNICAL TERMS

23. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite

contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed

properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

24. Based on my training, experience, and research, I know that devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, which can connect to the Internet, and therefore use an IP address. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

25. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

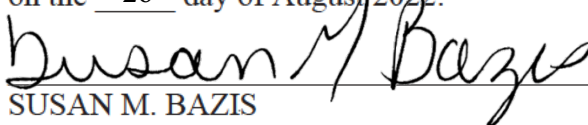
29. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the devices described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Timothy DuBois
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on the 26 day of August 2022:



SUSAN M. BAZIS
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is **One (1) Black Samsung cellular telephone with IMEI number 350319813108941** currently at FBI Omaha Headquarters located at 4411 S. 121st Street, Omaha, Nebraska 68137.

This warrant authorizes the forensic examination of the device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the devices described in Attachment A that relate to violations of federal law, including 18 U.S.C. § 2251(a) (sexual exploitation of children), 18 U.S.C. § 2252(a)(2) (receipt and distribution of child pornography), 18 U.S.C. § 2252(a)(1) (transportation of child pornography), 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2252A(a)(2)(A) (receipt and distribution of child pornography)

- a. Text messages, emails, conversations, and correspondence pertaining to the sexual exploitation of minors
- b. Communications related to the sexual exploitation of minors
- c. Photographs and/or Videos related to the sexual exploitation of minors;
- d. Records and information relating to sexual abuse and/or enticement of a minor;
- e. Records and information relating to the use of communication or social media platforms such as Instagram and Discord.

2. Visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same.

3. Passwords and other data security mechanisms designed to restrict access to or hide computer, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

4. Records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, including but not limited to social media accounts, cloud storage accounts, and email accounts, as well as any and all records relating to the ownership or use of

the computer hardware, digital device and/or digital media account.

5. Digital documents and records regarding the ownership and/or possession of the searched premises.

6. Electronic data contained in the Device regarding names, co-conspirators, associates, phone numbers, addresses, contact information, data, text, messages, images, voice memos, photographs, videos, internet sites, internet access, documents, emails and email accounts, social media accounts, cloud storage accounts, or other information, ledgers, contained in the cellular phone internal, external or removable memory or memories, which includes any smart cards, SIM cards or flash cards.

7. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

- a. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the
District of NebraskaIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 8:22MJ480

One (1) Black Samsung cellular telephone with IMEI number 350319813108941.
The device is currently located in the FBI Omaha Field Office, 4411 S.121st
Street, Omaha, Nebraska 68137, further described in Attachment A

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application presented by an attorney for the government requests the search of the following person or property
located in the _____ District of _____ Nebraska _____

(identify the person or describe the property to be searched and give its location)

One (1) Black Samsung cellular telephone with IMEI number 350319813108941. The device is currently located
in the FBI Omaha Field Office, 4411 S.121st Street, Omaha, Nebraska 68137, further described in Attachment AI find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before September 9, 2022 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to SUSAN M. BAZIS
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 8-26-22 at 5:00 p.m.


Judge's signature

City and state: Omaha, Nebraska

SUSAN M. BAZIS, U.S. Magistrate Judge
Printed name and title

SD/IA (Rev. 5/21) Search and Seizure Warrant (Page 2)

ReturnCase No.:
8:22MJ480

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

The property to be searched is **One (1) Black Samsung cellular telephone with IMEI number 350319813108941** currently at FBI Omaha Headquarters located at 4411 S. 121st Street, Omaha, Nebraska 68137.

This warrant authorizes the forensic examination of the device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the devices described in Attachment A that relate to violations of federal law, including 18 U.S.C. § 2251(a) (sexual exploitation of children), 18 U.S.C. § 2252(a)(2) (receipt and distribution of child pornography), 18 U.S.C. § 2252(a)(1) (transportation of child pornography), 18 U.S.C. § 2252(a)(4)(B) (possession of child pornography), 2252A(a)(5)(B) (possession of child pornography), and 2252A(a)(2)(A) (receipt and distribution of child pornography)

- a. Text messages, emails, conversations, and correspondence pertaining to the sexual exploitation of minors
- b. Communications related to the sexual exploitation of minors
- c. Photographs and/or Videos related to the sexual exploitation of minors;
- d. Records and information relating to sexual abuse and/or enticement of a minor;
- e. Records and information relating to the use of communication or social media platforms such as Instagram and Discord.

2. Visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same.

3. Passwords and other data security mechanisms designed to restrict access to or hide computer, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

4. Records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, including but not limited to social media accounts, cloud storage accounts, and email accounts, as well as any and all records relating to the ownership or use of

the computer hardware, digital device and/or digital media account.

5. Digital documents and records regarding the ownership and/or possession of the searched premises.

6. Electronic data contained in the Device regarding names, co-conspirators, associates, phone numbers, addresses, contact information, data, text, messages, images, voice memos, photographs, videos, internet sites, internet access, documents, emails and email accounts, social media accounts, cloud storage accounts, or other information, ledgers, contained in the cellular phone internal, external or removable memory or memories, which includes any smart cards, SIM cards or flash cards.

7. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

- a. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law

enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.